CLAIMS

1. Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:

an encryption execution unit contained within the pipelined processor; and

a software and hardware interface that enables the encryption execution unit to efficiently cooperate with resources of the pipelined processor.

2. The apparatus of Claim 1 wherein the encryption execution unit is an encryption tightly coupled state machine (TCSM) unit that is selectively invoked within the pipelined processor.

3. The apparatus of Claim 2 wherein a software portion of the interface comprises native encryption opcodes provided within an instruction set of the pipelined processor to enable selective access to the encryption TCSM unit.

4. The apparatus of Claim 3 wherein the resources include a plurality of busses internal to the pipelined processor and wherein a hardware portion of the interface allows the encryption TCSM unit to utilize the internal buses in response to decode processing of the native encryption opcodes.

5. The apparatus of Claim 4 wherein the pipelined processor is microcontroller core (TMC) processor having a multi-stage pipeline architecture that includes an instruction fetch stage, an instruction decode stage, an execution stage and a memory write-back stage.

6. The apparatus of Claim 5 wherein the TMC processor further includes an arithmetic logic unit, at least one internal register, an instruction fetch and decode unit and the encryption TCSM unit organized as a data path.

7. The apparatus of Claim 5 wherein the encryption TCSM unit comprises a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

8. The apparatus of Claim 7 wherein the DES functional component comprises state machine hardware used to execute each round of a DES function.

9. The apparatus of Claim 7 wherein the sub-key generation functional component comprises state machine hardware that generates a sub-key as needed for each round of the DES function.

10. A method for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the method comprising the steps of:

providing an encryption execution unit within the pipelined processor; and

selectively accessing the encryption execution unit through an integrated hardware and software interface of the pipelined processor that allows efficient cooperation between the encryption execution unit and resources of the pipelined processor.

11. The method of Claim 10 wherein the integrated interface comprises native encryption opcodes contained within an instruction set of the pipelined processor and wherein the step of selectively accessing comprises the step of issuing the native encryption opcodes directly to the encryption execution unit to substantially reduce encryption setup latency.

12. The method of Claim 11 further comprising the steps of, wherein the pipelined processor is a microcontroller core (TMC) processor having a multi-stage pipeline architecture that includes an instruction decode stage and an execution stage:

decoding the native encryption opcodes at the instruction decode stage; and

in response to the step of decoding, invoking the encryption execution unit to perform encryption/decryption functions at the execution stage.

13. The method of Claim 12 further comprising the steps of, wherein the encryption/decryption functions are performed on plaintext stored at the network switch:

protocol processing of protocols contained in the plaintext to determine an appropriate encryption algorithm;

upon determining the appropriate encryption algorithm, immediately starting an operation to fetch initial keys needed to perform the encryption/decryption functions; and

upon fetching the keys, providing the keys to the encryption execution unit within the TMC processor.

14. The method of Claim 13 wherein the resources include a plurality of high-performance busses internal to the TMC processor, and wherein the step of invoking comprises the step of:

accessing the internal busses through the integrated interface to simultaneously load an encryption key and store a previous encryption result.

15. The method of Claim 12 further comprising the step of, wherein the the encryption execution unit is an encryption tightly coupled state machine (TCSM) unit:

initializing the encryption TCSM unit in response to execution of a first instruction that defines the form of operation to be performed.

16. The method of Claim 15 wherein the encryption TCSM unit comprises a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component and wherein the step of initializing comprises the steps of:

decoding a first portion of the first instruction to initialize the DES functional component; and

decoding a second portion of the first instruction to initialize the sub-key generation functional component.

17. The method of Claim 16 further comprising the step of:

executing a second instruction having a micro-opcode field containing a native encryption opcode that specifies loading an initial key from a memory into the sub-key generation functional component of the encryption TCSM unit.

18. The method of Claim 17 further comprising the step of:

performing a DES function on the plaintext in response to execution of a third instruction having a micro-opcode field containing a native encryption code that specifies loading of the plaintext into the DES functional component of the encryption TCSM unit and initiating DES operations; and

upon completing the DES operations, storing ciphertext results in an internal register coupled to the DES functional component.

19. The method of Claim 18 further comprising the step of:

executing a fourth instruction to store the ciphertext results contained in the internal register to a location in the memory.

20. A programmable processing engine of a network switch comprising:

an input header buffer;

an output header buffer; and

a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked through an integrated hardware and software interface of the microcontroller core to allow efficient cooperation between the encryption TCSM unit and data path resources of the microcontroller core.